PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-197078
(43)Date of publication of application : 15.07.1994

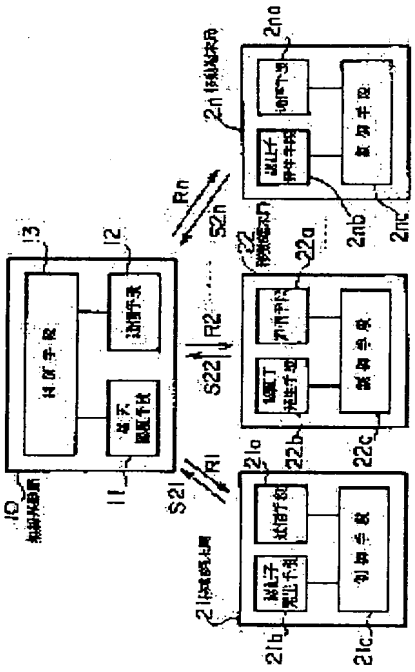
(51)Int.Cl. H04B 7/26
H04L 9/06
H04L 9/14

(21)Application number : 04-344762
(22)Date of filing : 24.12.1992

(71)Applicant : FUJITSU LTD
(72)Inventor : TORII NAOYA
AKIYAMA RYOTA

(54) COMMUNICATION TERMINAL EQUIPMENT CONNECTION SYSTEM

(57)Abstract:
PURPOSE: To identify a mobile terminal equipment station by allowing even a conventional portable radio communication equipment to execute ciphering and decoding processing in a short time.
CONSTITUTION: A terminal equipment identification means 11 of a radio base station 10 has a different secret key K21 from a mobile terminal equipment station 21 or the like and generates and outputs a 1st random number series R1 or the like and compares 1st and 2nd identifiers S21, S22 obtained by the inner product between the secret key or the like and the 1st random number series R1 or the like to output a prescribed allowable signal. Furthermore, a 1st radio communication means 12 sends the 1st random number string or the like and receives the 2nd identifier S21 or the like. A 2nd radio communication means 21a or the like in a mobile terminal equipment station 21 receives the 1st random number series R1 or the like and sends the 2nd identifier S21 or the like. Furthermore, an identifier generating means 21b or the like has a secret key K21 or the like and outputs a 2nd identifier S21 or the like obtained by the inner product between a secret key K21 or the like and the 1st random number series R1 or the like.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－197078

(43)公開日　平成6年（1994）7月15日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｂ	7/26	１０９	Ｓ　7304－5Ｋ			
Ｈ０４Ｌ	9/06					
	9/14					
			7117－5Ｋ	Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数８（全 20 頁）

(21)出願番号　特願平4－344762

(22)出願日　平成4年（1992）12月24日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　鳥居　直哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

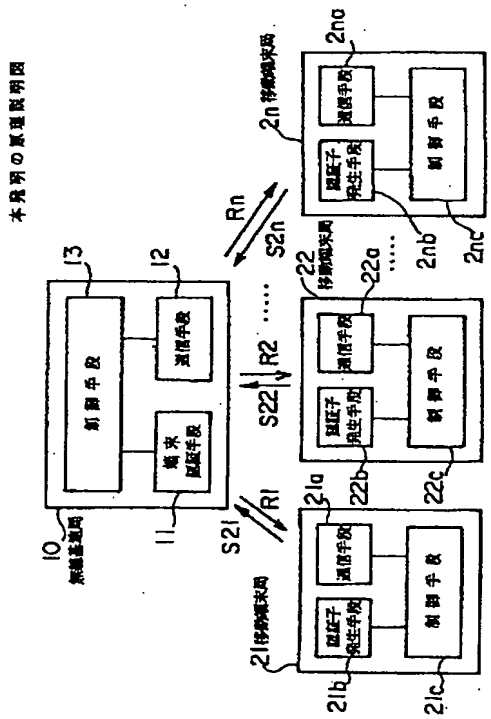
(74)代理人　弁理士　井桁　貞一

(54)【発明の名称】通信端末接続方式

(57)【要約】

【目的】　通信端末接続方式に関し、従来の携帯用無線通信装置であっても暗号化及び復号化処理を短時間で行い、移動端末局の認証を行うことを目的とする。

【構成】　無線基地局１０において、端末認証手段１１は移動端末局２１等ごとに異なる秘密鍵Ｋ２１等を有し、第１の乱数列Ｒ１等を発生して出力するとともに、秘密鍵Ｋ２１等と第１の乱数列Ｒ１等との内積により求めた第１の認証子Ｓ１１等と第２の認証子Ｓ２１等とを比較して所定の許否信号を出力する。また、第１の無線通信手段１２は第１の乱数列Ｒ１等を送信するとともに、第２の認証子Ｓ２１等を受信する。移動端末局２１において、第２の無線通信手段２１ａ等は第１の乱数列Ｒ１等を受信するとともに、第２の認証子Ｓ２１等を送信する。また、認証子発生手段２１ｂ等は秘密鍵Ｋ２１等を有し、この秘密鍵Ｋ２１等と第１の乱数列Ｒ１等との内積により求めた第２の認証子Ｓ２１等を出力する。



1

【特許請求の範囲】

【請求項1】　無線基地局と移動端末局との間で通信許可を付与するための認証を行う通信端末接続方式において、

移動端末局（21，22，・・・，2n）ごとに異なる秘密鍵（K21，K22，・・・，K2n）を有し、第1の乱数列（R1，R2，・・・，Rn）を発生して出力するとともに、前記秘密鍵（K21，K22，・・・，K2n）と出力した前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求められる第1の認証子（S11，S12，・・・，S1n）と、第2の認証子（S21，S22，・・・，S2n）とを比較して所定の許否信号を出力する端末認証手段（11）と、前記第1の乱数列（R1，R2，・・・，Rn）を送信するとともに前記第2の認証子（S21，S22，・・・，S2n）を受信する第1の無線通信手段（12）とを備えた無線基地局（10）と、

前記第1の乱数列（R1，R2，・・・，Rn）を受信するとともに前記第2の認証子（S21，S22，・・・，S2n）を送信する第2の無線通信手段（21a，22a，・・・，2na）と、前記秘密鍵（K21，K22，・・・，K2n）の一つを有し、前記秘密鍵（K21，K22，・・・，K2n）の一つと受信した前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求めた前記第2の認証子（S21，S22，・・・，S2n）を出力する認証子発生手段（21b，22b，・・・，2nb）とを備えた移動端末局（21，22，・・・，2n）と、

を有することを特徴とする通信端末接続方式。

【請求項2】　前記前記認証子発生手段（21b，22b，・・・，2nb）は第2の乱数列（R21，R22，・・・，R2n）を発生する乱数発生手段、をさらに備えたことを特徴とする請求項1記載の通信端末接続方式。

【請求項3】　前記端末認証手段（11）は、前記秘密鍵（K21，K22，・・・，K2n）と前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求めた後、前記秘密鍵（K21，K22，・・・，K2n）に基づく位置から所定の長さのデータを前記第1の認証子（S11，S12，・・・，S1n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

【請求項4】　前記端末認証手段（11）は、前記秘密鍵（K21，K22，・・・，K2n）と前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求めた後、前記秘密鍵（K21，K22，・・・，K2n）に基づいて転置処理を行なったデータを前記第1の認証子（S11，S12，・・・，S1n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

2

【請求項5】　前記端末認証手段（11）は、前記秘密鍵（K21，K22，・・・，K2n）に基づいて前記第1の乱数列（R1，R2，・・・，Rn）を転置処理した後、前記秘密鍵（K21，K22，・・・，K2n）との内積を演算して求めたデータを前記第1の認証子（S11，S12，・・・，S1n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

【請求項6】　前記認証子発生手段（21b，22b，・・・，2nb）は、前記秘密鍵（K21，K22，・・・，K2n）と前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求めた後、前記秘密鍵（K21，K22，・・・，K2n）に基づく位置から所定の長さのデータを前記第2の認証子（S21，S22，・・・，S2n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

【請求項7】　前記認証子発生手段（21b，22b，・・・，2nb）は、前記秘密鍵（K21，K22，・・・，K2n）と前記第1の乱数列（R1，R2，・・・，Rn）との内積を演算して求めた後、前記秘密鍵（K21，K22，・・・，K2n）に基づいて転置処理を行なったデータを前記第2の認証子（S21，S22，・・・，S2n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

【請求項8】　前記端末認証手段（21b，22b，・・・，2nb）は、前記秘密鍵（K21，K22，・・・，K2n）に基づいて前記第1の乱数列（R1，R2，・・・，Rn）を転置処理した後、前記秘密鍵（K21，K22，・・・，K2n）との内積を演算して求めたデータを前記第2の認証子（S21，S22，・・・，S2n）とするように構成したことを特徴とする請求項1又は請求項2記載の通信端末接続方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は無線通信局間の通信端末接続方式に関し、特に無線基地局と移動端末局との間で通信許可を付与するための認証を行う通信端末接続方式に関する。

【0002】近年、人・自動車・船舶・列車・飛行機等の移動体を対象とする移動通信が急速に実用化されつつある。この移動通信では、通信を行うための場所が特定されないため、任意の場所で通信を行うことができるという利点がある。特に、昭和54年にサービスが開始された自動車電話や昭和62年にサービスが開始された携帯電話機等の普及は、高度情報社会にとって欠かせないサービスになりつつある。

【0003】一般に、移動体に無線通信設備を設けた端末装置を「移動端末局」と呼ぶ。この移動端末局には、警察・消防・救急等の公共移動端末局や、列車・タクシー等の民間移動端末局がある。また、警察庁や車両管理

センター等のように、管理の対象となる移動端末局を掌握するための集中管理局を「無線基地局」と呼ぶ。

【0004】ところで、無線基地局と移動端末局との間で無線通信を行う場合、通信接続を希望する移動端末局が無線基地局に登録されている正規の移動端末局であるか否かを判別する必要がある。この判別によって移動端末局の正当性を証明することを「認証（authentication）」と呼ぶ。そして、移動端末局は認証を受けるために、無線基地局へ移動端末局ごとに付された固有の「ＩＤ（IDentity）」と呼ばれる識別符号を伝送する。

【0005】したがって、他の無線機等で上記識別符号が傍受されても、その内容が分からないようにするため、暗号化して伝送する必要がある。

【0006】

【従来の技術】従来は、上記の暗号化処理に、アメリカ合衆国の連邦規格となっているＤＥＳ（Data Encryption Standard）方式を用いて行なっていた。ＤＥＳ方式は、同一の鍵又は一方から他方が容易に導ける鍵の対を用いる暗号の方式である「共通鍵方式（common key system）」の一つであって、乱数、換字及び転置を複雑に組み合わせた方式である。ここで、換字は鍵によって指定された方法で文字を他の文字で置き換える手順であり、転置は文字の順序を入れ換える手順である。

【0007】上記ＤＥＳ方式では、６４〔ビット〕の単位で変換が行われる。このように、数十〔ビット〕以上の暗号を変換する処理単位を「ブロック暗号（block cipher）」と呼ぶ。

【0008】したがって、ＤＥＳ方式によって暗号化された識別符号が他の無線機等で傍受されても、復号化が複雑なために解読するのはほぼ不可能であった。このため、移動端末局の認証で安全に使用することができた。

【0009】

【発明が解決しようとする課題】しかし、ＤＥＳ方式では暗号化及び復号化処理における処理量が膨大であるため、特に外形が制限される小型の携帯用無線通信装置では多くの処理時間が必要になり、場合によっては専用のハードウェアを必要としていた。このため、コストが高くなるという問題点があった。

【0010】本発明はこのような点に鑑みてなされたものであり、従来の携帯用無線通信装置であっても暗号化及び復号化処理が短時間で行え、移動端末局の認証を行う通信端末接続方式を、提供することを目的とする。

【0011】

【課題を解決するための手段】図１は上記目的を達成する本発明の原理説明図である。本発明の通信端末接続方式は無線基地局１０と移動端末局２１，２２，・・・，２ｎとからなり、無線基地局１０は端末認証手段１１及び第１の無線通信手段１２を備え、移動端末局２１，２２，・・・，２ｎはそれぞれ第２の無線通信手段２１ａ，２２ａ，・・・，２ｎａ及び認証子発生手段２１ｂ，２２ｂ，・・・，２ｎｂを備える。

【0012】無線基地局１０において、端末認証手段１１は移動端末局２１，２２，・・・，２ｎごとに異なる秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎを有し、第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎを発生して出力するとともに、上記秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎと出力した第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎとの内積を演算して求められる第１の認証子Ｓ１１，Ｓ１２，・・・，Ｓ１ｎと、後述する第１の無線通信手段１２で受信した第２の認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎとを比較して所定の許否信号を出力する。また、第１の無線通信手段１２は第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎを送信するとともに、第２の認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎを受信する。

【0013】移動端末局２１において、第２の無線通信手段２１ａは第１の乱数列Ｒ１を受信するとともに、第２の認証子Ｓ２１を送信する。また、認証子発生手段２１ｂは上記秘密鍵Ｋ２１を有し、この秘密鍵Ｋ２１と受信した第１の乱数列Ｒ１との内積を演算して求めた第２の認証子Ｓ２１を出力する。

【0014】同様に、移動端末局２２，・・・，２ｎにおいて、第２の無線通信手段２２ａ，・・・，２ｎａはそれぞれ第１の乱数列Ｒ２，・・・，Ｒｎを受信するとともに、第２の認証子Ｓ２２，・・・，Ｓ２ｎをそれぞれ送信する。また、認証子発生手段２２ｂ，・・・，２ｎｂはそれぞれ秘密鍵Ｋ２２，・・・，Ｋ２ｎを有し、この秘密鍵Ｋ２２，・・・，Ｋ２ｎと受信した第１の乱数列Ｒ２，・・・，Ｒｎとの内積を演算して求めた第２の認証子Ｓ２２，・・・，Ｓ２ｎをそれぞれ出力する。

【0015】

【作用】無線基地局１０において、まず端末認証手段１１が第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎを発生して出力し、第１の無線通信手段１２がこの第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎを送信する。

【0016】そして、移動端末局２１，２２，・・・，２ｎにおいて、第２の無線通信手段２１ａ，２２ａ，・・・，２ｎａがそれぞれ第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎを受信すると、認証子発生手段２１ｂ，２２ｂ，・・・，２ｎｂはそれぞれ秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎの一つと受信した第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎとの内積を演算して第２の認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎをそれぞれ求める。こうして求められた第２の認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎは、第２の無線通信手段２１ａ，２２ａ，・・・，２ｎａによってそれぞれ送信される。

【0017】さらに、無線基地局１０において、第１の無線通信手段１２が第２の認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎを受信すると、端末認証手段１１が秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎと、最初に出力した第１の乱数列Ｒ１，Ｒ２，・・・，Ｒｎとの内積を演算して

5

第1の認証子S11，S12，・・・，S1nを求める。その後、端末認証手段11は第1の認証子S11，S12，・・・，S1nと受信した第2の認証子S21，S22，・・・，S2nとを比較して所定の許否信号を出力する。

【0018】

【実施例】以下、本発明の一実施例を図面に基づいて説明する。図1は本発明の原理説明図であるとともに、実施例を示す図である。本発明の通信端末接続方式は無線基地局10と移動端末局21，22，・・・，2nとからなり、無線基地局10は端末認証手段11、無線通信手段12及び制御手段13を備え、移動端末局21，22，・・・，2nはそれぞれ無線通信手段21a，22a，・・・，2na、認証子発生手段21b，22b，・・・，2nb及び制御手段21c，22c，・・・，2ncを備える。

【0019】無線基地局10において、端末認証手段11は通信接続可能な移動端末局21，22，・・・，2nごとに異なる秘密鍵K21，K22，・・・，K2nを後述する秘密鍵データベースに有し、乱数列R1，R2，・・・，Rnを発生して出力する。また、移動端末局21，22，・・・，2nは、この秘密鍵K21，K22，・・・，K2nと出力した乱数列R1，R2，・・・，Rnとの内積を演算して求められる認証子S11，S12，・・・，S1nと、無線通信手段12で受信した認証子S21，S22，・・・，S2nとを比較して所定の許否信号、具体的には通信許可又は通信拒否の信号を出力する。無線通信手段12は乱数列R1，R2，・・・，Rnを送信するとともに、認証子S21，S22，・・・，S2nを受信する。また、制御手段13は無線基地局10全体を制御するとともに、端末認証手段11及び無線通信手段12の動作制御を行う。

【0020】なお、乱数列R1，R2，・・・，Rnは例えば128〔ビット〕の符号列であり、秘密鍵K21，K22，・・・，K2n及び認証子S21，S22，・・・，S2n等は例えば64〔ビット〕の符号列である。

【0021】移動端末局21において、無線通信手段21aは乱数列R1を受信するとともに、認証子S21を送信する。認証子発生手段21bは秘密鍵K21を有し、この秘密鍵K21と受信した乱数列R1との内積を演算して求めた認証子S21を出力する。制御手段21cは移動端末局21全体を制御するとともに、無線通信手段21a及び認証子発生手段21bの動作制御を行う。

【0022】同様に、移動端末局22，・・・，2nにおいて、無線通信手段22a，・・・，2naはそれぞれ乱数列R2，・・・，Rnを受信するとともに、認証子S22，・・・，S2nをそれぞれ送信する。また、認証子発生手段22b，・・・，2nbはそれぞれ秘密

6

鍵K22，・・・，K2nの一つを有し、この秘密鍵K22，・・・，K2nの一つと受信した乱数列R2，・・・，Rnとの内積を演算して求めた認証子S22，・・・，S2nをそれぞれ出力する。また、制御手段22c，・・・，2ncは、それぞれ移動端末局22，・・・，2n全体を制御するとともに、無線通信手段22a，・・・，2na及び認証子発生手段22b，・・・，2nbの動作制御を行う。

【0023】次に、本発明の通信端末接続方式の動作について説明する。なお、無線基地局10と移動端末局21との間、無線基地局10と移動端末局22との間、・・・、無線基地局10と移動端末局2nとの間は、いずれも同様な動作をなすので、ここでは無線基地局10と移動端末局21との間の動作について説明する。

【0024】無線基地局10では、まず端末認証手段11が乱数列R1を発生して出力し、無線通信手段12がこの乱数列R1を送信する。そして、移動端末局21では、無線通信手段21aが乱数列R1を受信すると、認証子発生手段21bは秘密鍵K21と受信した乱数列R1との内積を演算して認証子S21を求める。こうして求められた認証子S21は、無線通信手段21aによって送信される。

【0025】さらに、無線基地局10では、無線通信手段12が移動端末局21から送信された認証子S21を受信すると、端末認証手段11が秘密鍵K21と上記出力した乱数列R1との内積を演算して認証子S11を求める。その後、端末認証手段11は演算して求めた認証子S11と受信した認証子S21とを比較して所定の許否信号YNを出力する。具体的には、認証子S11と認証子S21とが一致した場合は通信許可の信号を出力し、そうでない場合は通信拒否の信号を出力する。

【0026】次に、無線基地局10の端末認証手段11、及び移動端末局21の認証子発生手段21bの具体的な構成について説明する。図2は端末認証手段11の構成を示すブロック図である。端末認証手段11は、秘密鍵データベース11a、乱数発生手段11b、出力手段11c、演算手段11d、後処理手段11e、入力手段11f及び比較手段11gの各要素から構成される。

【0027】秘密鍵データベース11aは通信接続可能な移動端末局21，22，・・・，2nごとに異なる秘密鍵K21，K22，・・・，K2nを格納する。乱数発生手段11bは図1の制御手段13からの指令に応じて、例えば日付・時刻によって変化する乱数列R1，R2，・・・，Rnを発生する。出力手段11cは乱数発生手段11bで発生した乱数列R1，R2，・・・，Rn及び後述する比較手段11gから出力された所定の許否信号YNを一定の出力レベルに増幅して出力する。

【0028】演算手段11dは、秘密鍵データベース11aに格納された秘密鍵K21，K22，・・・，K2nと、乱数発生手段11bで発生した乱数列R1，R

2，・・・，Ｒｎとの内積をそれぞれ演算して内積列ＭＳ１１，ＭＳ１２，・・・，ＭＳ１ｎを求める。後処理手段１１ｅは、演算手段１１ｄで求められた内積列ＭＳ１１，ＭＳ１２，・・・，ＭＳ１ｎについて、上記秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎに基づいて後述する後処理を行い、認証子Ｓ１１，１２，・・・，Ｓ１ｎを求めて出力する。入力手段１１ｆは図１の通信手段１２によって受信された認証子Ｓ２１，２２，・・・，Ｓ２ｎを受ける。

【００２９】比較手段１１ｇは後処理手段１１ｅから出力された認証子Ｓ１１，１２，・・・，Ｓ１ｎと、入力手段１１ｆから出力された認証子Ｓ２１，２２，・・・，Ｓ２ｎとを比較して、所定の許否信号ＹＮを出力する。具体的には、認証子Ｓ１１，１２，・・・，Ｓ１ｎと、入力手段１１ｆから出力された認証子Ｓ２１，２２，・・・，Ｓ２ｎとが一致した場合は通信許可の信号を出力し、そうでない場合は通信拒否の信号を出力する。

【００３０】図３は認証子発生手段の構成を示すブロック図である。なお、認証子発生手段２１ｂ，２２ｂ，・・・，２ｎｂはいずれも同一構成であるので、ここでは認証子発生手段２１ｂの構成について説明する。

【００３１】認証子発生手段２１ｂは入力手段２１ｂａ、演算手段２１ｂｂ、秘密鍵データ２１ｂｃ、後処理手段２１ｂｄ及び出力手段２１ｂｅの各要素から構成される。入力手段２１ｂａ、図１の通信手段２１ａによって受信された乱数列Ｒ１を受ける。演算手段２１ｂｂは後述する秘密鍵データ２１ｂｃと、受信した乱数列Ｒ１との内積を演算して内積列ＭＳ２１を求める。秘密鍵データ２１ｂｃは例えばＥＥＰＲＯＭ等の記憶装置に所定の形式で格納されたデータであって、図２の秘密鍵データベース１１ａに格納された秘密鍵Ｋ２１と同一である。後処理手段２１ｂｄは演算手段２１ｂｂで求められた内積列ＭＳ２１について、上記秘密鍵データ２１ｂｃに基づいて後述する後処理を行い、認証子Ｓ２１を求めて出力する。出力手段２１ｂｅは、後処理手段２１ｂｄから出力された認証子Ｓ２１を一定の出力レベルに増幅して出力する。

【００３２】次に、上記後処理手段１１ｅ又は後処理手段２１ｂｄ等で行われる後処理について説明する。図４は認証子の決定方法の一例を示す図であり、図４（Ａ）には内積列ＭＳｉの一例を示し、図４（Ｂ）には鍵Ｋｘと認証子Ｓｉとの関係を示す。なお、ここでは説明を簡単にするために、内積列ＭＳｉを１６〔ビット〕、認証子Ｓｉを８〔ビット〕と規定する。以下、図及び書面上でビット列を見やすくするために、４〔ビット〕ごとに空白を挿入する。

【００３３】図４（Ａ）において、内積列２００は演算手段１１ｄ又は演算手段２１ｂｂ等で演算された結果を示す１６〔ビット〕の符号列である。ここで、内積列２００は上記の通り１６〔ビット〕と規定したので、認証子Ｓｉを抽出するために鍵Ｋｘとして必要なビット数は$\log_2 16 = 4$〔ビット〕である。ここでは、内積列２００の先頭の４〔ビット〕のデータ、すなわち「１０１１」を鍵２０１としている。

【００３４】そして、後処理として、鍵２０１で指定された４〔ビット〕を数値化し、この数値化されたビット位置から８〔ビット〕の符号列を認証子Ｓｉとして抽出する。こうして抽出された認証子Ｓｉと、鍵Ｋｘとの関係を図４（Ｂ）に示す。

【００３５】図４（Ｂ）において、関係テーブル３００は図４（Ａ）の内積列２００における鍵Ｋｘと認証子Ｓｉとの関係を示すテーブルである。関係テーブル３００の左欄に鍵Ｋｘを、右欄に認証子Ｓｉを示す。

【００３６】もし、鍵Ｋｘが「００００」ならば、３０１行に示すように、内積列２００から抽出される認証子Ｓｉは内積列２００の第１ビット目（左端）から８〔ビット〕の符号列「１０１１１１１０」となる。同様に、鍵Ｋｘが「０００１」ならば、３０２行に示すように、内積列２００から抽出される認証子Ｓｉは内積列２００の第２ビット目から８〔ビット〕の符号列「０１１１１１００」となる。また、鍵Ｋｘが「００１０」ならば、３０３行に示すように、認証子Ｓｉは内積列２００の第３ビット目から８〔ビット〕の符号列「１１１１１０００」となる。さらに、鍵Ｋｘが「００１１」ならば、３０４行に示すように、「１１１１０００１」となる。なお、抽出する８〔ビット〕の符号列が第１６ビット目を超える場合は、さらに内積列２００の第１ビット目から続けて抽出する。

【００３７】したがって、図４（Ａ）の内積列２００における鍵Ｋｘは「１０１１」であるので、抽出される認証子Ｓｉは３０５行に示すように、内積列２００の第１１ビット目から８〔ビット〕の符号列「０１００００１」となる。

【００３８】上記の後処理の例では、内積列２００の第１ビット目を先頭ビットとして、鍵Ｋｘのビット位置から８〔ビット〕の符号列を抽出するように構成したが、内積列２００の第８ビット目を先頭ビットとする等のように、所定の第８ビット目を先頭ビットとして鍵Ｋｘのビット位置から８〔ビット〕の符号列を抽出するように構成することもできる。また、符号列の抽出は内積列２００の図面左側から右側へ向かって行なったが、逆に内積列２００の図面右側から左側へ向かって抽出するように構成してもよい。

【００３９】図５は転置処理の一例を示す図である。ここにいう転置処理とは、認証子Ｓ２１，Ｓ２２等の認証子Ｓｉのように指定された符号列内の符号の順位を入れ換える操作である。なお、ここでは転置処理の対象となる認証子Ｓｉを８〔ビット〕の符号列「B_7 B_6 B_5 B_4 B_3 B_2 B_1 B_0」（B_7，B_6，B_5等は「０」又は「１」）と仮定

する。また、鍵Kx は図4で説明したように規定される符号列であって、ここでは17ビットの符号列「0010 0110 1110 1010 1」が与えられているものと仮定する。鍵データKd は、鍵Kx のうち転置処理に必要なビット数の符号列である。

【0040】ここで、転置処理の対象となる認証子Si は8〔ビット〕であるので、ビット位置を指定するために必要なビット数は $\log_2 8=3$〔ビット〕である。したがって、最初の転置処理に使用される鍵データKd は、上記鍵Kx の先頭から3〔ビット〕の符号列「001」である。

【0041】そして、認証子Si 内の符号の順位の入れ換えは、鍵Kx の符号列を数値化した後に1を足し、このビット位置の符号から順に抽出して新たな符号列を作成する。

【0042】具体的には、最初の転置処理に使用される鍵データKd は401行に示すように「001」であるので、符号列「B_7 B_6 B_5 B_4 B_3 B_2 B_1 B_0 」のうち2番目の符号「B_6」を抽出する。なお、符号「B_6」が抽出されると、認証子Si の符号列から符号「B_6」がなくなり、符号列「B_7 B_5 B_4 B_3 B_2 B_1 B_0」となる。

【0043】同様に、転置処理の対象となる符号列は7〔ビット〕であるので、ビット位置を指定するために必要なビット数は $\log_2 7$、すなわち3〔ビット〕である。よって、2回目の転置処理に使用される鍵データKd は402行に示すように、鍵Kx の第4ビット目からの3〔ビット〕の符号列「001」である。したがって、符号列「B_7 B_5 B_4 B_3 B_2 B_1 B_0」のうち2番目の符号「B_5」を抽出する。なお、符号「B_5」が抽出されると符号「B_5」がなくなり、認証子Si の符号列は「B_7 B_4 B_3 B_2 B_1 B_0 」となる。また、新たな符号列は「B_6 B_5 」になる。

【0044】さらに、転置処理の対象となる符号列が403行に示すように4〔ビット〕になると、ビット位置を指定するために必要なビット数は $\log_2 4$、すなわち2〔ビット〕である。よって、5回目の転置処理に使用される鍵データKd は鍵Kx の第13ビット目からの2〔ビット〕の符号列「10」である。したがって、符号列「B_7 B_3 B_2 B_1 」のうち3番目の符号「B_2」を抽出する。なお、符号「B_2」が抽出されると符号「B_2」がなくなり、認証子Si の符号列は「B_7 B_3 B_1」となる。また、新たな符号列は「B_6 B_5 B_0 B_4 B_2」になる。

【0045】このような手続きによって、最終的には404行に示すように新たな符号列、すなわち認証子Si の符号列は「B_6 B_5 B_0 B_4 B_2 B_3 B_1 B_7 」となる。このように、転置処理の対象となる符号列の符号を入れ換えることによって、認証子Si等の符号列が傍受されても、その内容を解析することは困難であるので、通信内容の秘密性を確保することができる。

【0046】次に、本発明を実施するための処理手順について説明する。

【0047】図6は無線基地局10側の処理手順を示すフローチャートである。図において、Sの後に続く数字はステップ番号を示す。なお、無線基地局10と移動端末局21との間、無線基地局10と移動端末局22との間、・・・、無線基地局10と移動端末局2nとの間は、いずれも同様の処理手順であるので、ここでは図1と同様に無線基地局10と移動端末局21との間の処理手順について説明する。

〔S61〕乱数列を発生する。具体的には、図2に示す乱数発生手段11bによって乱数列R1を発生し、出力手段11cによって所定の出力レベルに増幅して出力する。

〔S62〕ステップS61で発生した乱数列を送信する。すなわち、ディジタルデータとしての乱数列R1を、図1の通信手段12が無線電波に変換して出力する。

〔S63〕認証子を受信する。ステップS62で出力された乱数列R1を移動端末局21が受信すると、認証子S21を演算して無線電波で送信する。このため、移動端末局21から送信された認証子S21を受信する。

〔S64〕秘密鍵を取得する。具体的には、図2の秘密鍵データベース11aから通信の対象となる移動端末局21に対応した秘密鍵K21を取得する。

〔S65〕内積演算を行う。具体的には後述するように、ステップS61で発生した乱数列R1と、ステップS64で取得した秘密鍵K21とから内積を演算して、内積列MS11を求める。

〔S66〕後処理を行う。具体的には、ステップS65で求められた内積列MS11に基づいて、後述する図9に示す抽出処理又は後述する図10に示す転置処理を行なって、認証子S11を求める。

〔S67〕受信認証子との比較を行う。すなわち、ステップS63で受信した移動端末局21の認証子S21と、ステップS66で求められた認証子S11とを比較する。

〔S68〕移動端末局21が無線基地局10に正規に登録された端末局か否かを判別する。具体的には、ステップS63で受信した移動端末局21の認証子S21と、ステップS66で求められた認証子S11とが一致するか否かを判別する。もし、認証子S21と認証子S11とが一致する（YES）ならば本処理手順を終了し、そうでない（NO）ならばステップS61に戻る。

【0048】図7は移動端末局側の処理手順を示すフローチャートである。なお、図1に示す認証子発生手段21b，22b，・・・，2nbの処理手順はいずれも同一であるので、ここでは認証子発生手段21bの処理手順について説明する。図において、Sの後に続く数字はステップ番号を示す。

〔S71〕乱数列を受信する。すなわち、図1の無線基

地局１０から送信された乱数列Ｒ１を通信手段２１ａが受信し、図３の入力手段２１ｂａがこの乱数列Ｒ１を受ける。

〔Ｓ７２〕秘密鍵を取得する。具体的には、図３の演算手段２１ｂｂが秘密鍵データ２１ｂｃを取得する。なお、この秘密鍵データ２１ｂｃは、図６のステップＳ６４で示した移動端末局２１に対応する秘密鍵Ｋ２１と同一のデータである。

〔Ｓ７３〕内積演算を行う。具体的には後述するように、ステップＳ７１で受けた乱数列Ｒ１と、ステップＳ７２で取得した秘密鍵データ２１ｂｃとから内積を演算して、内積列ＭＳ２１を求める。

〔Ｓ７４〕後処理を行う。具体的には、ステップＳ６５で求められた内積列ＭＳ２１に基づいて、後述する図９に示す抽出処理又は後述する図１０に示す転置処理を行なって、認証子Ｓ２１を求める。

〔Ｓ７５〕ステップＳ７４で求められた認証子Ｓ２１を送信する。すなわち、ディジタルデータとしての認証子Ｓ２１を、通信手段２１ａが無線電波に変換して出力する。

【００４９】次に、上記図６及び図７に示す内積演算処理及び後処理の具体的な処理手順について、図８乃至図１０で説明する。なお、無線基地局１０の演算手段１１ｄ及び移動端末局２１，２２，・・・，２ｎの演算手段２１ｂｂ，２２ｂｂ，・・・，２ｎｂｂにおいては同様の処理手順で行われるので、これらの図面の説明では移動端末局２１の演算手段２１ｂｂにおいて行われる処理手順について説明する。

【００５０】図８は内積演算の処理手順を示すフローチャートである。図において、Ｓの後に続く数字はステップ番号を示す。

〔Ｓ８１〕初期化処理を行う。すなわち、変数ｊ及び内積列ＭＳ２１を初期化する。具体的には、変数ｊに「１」を、乱数列ＭＳ２１に「０」を代入する。

〔Ｓ８２〕内積演算を行う。具体的には、秘密鍵Ｋ２１のｊ番目のビット（Ｋ２１ｊ）と乱数列Ｒ２のｊ番目のビット（Ｒ２ｊ）との積を、内積列ＭＳ２１のｊ番目のビット（ＭＳ２１ｊ）として代入する。

〔Ｓ８３〕インクリメント処理を行う。すなわち、変数ｊの値を１だけ増す。

〔Ｓ８４〕処理の終了か否かを判別する。すなわち、変数ｊの値が所定の数ｎを超えたか否かを判別する。もし、変数ｊの値が所定の数ｎを超えた（ＹＥＳ）ならば本処理手順を終了し、そうでない（ＮＯ）ならばステップＳ８２に戻る。

【００５１】図９は後処理の処理手順を示すフローチャートである。図において、Ｓの後に続く数字はステップ番号を示す。

〔Ｓ９１〕秘密鍵を取得する。具体的には、図３の演算手段２１ｂｂが秘密鍵データ２１ｂｃを取得する。な

お、この秘密鍵データ２１ｂｃは、図６のステップＳ６４で示した移動端末局２１に対応する秘密鍵Ｋ２１と同一のデータである。

〔Ｓ９２〕認証子を抽出する。すなわち、図７のステップＳ７４で求められた内積列ＭＳ２１に基づいて、認証子Ｓ２１の抽出処理を行う。具体的には、図４に示す認証子の決定方法に基づいて、認証子Ｓ２１の抽出処理を行う。

【００５２】図１０は他の後処理の処理手順を示すフローチャートである。図において、Ｓの後に続く数字はステップ番号を示す。

〔Ｓ１０１〕秘密鍵を取得する。具体的には、図３の演算手段２１ｂｂが秘密鍵データ２１ｂｃを取得する。なお、この秘密鍵データ２１ｂｃは、図６のステップＳ６４で示した移動端末局２１に対応する秘密鍵Ｋ２１と同一のデータである。

〔Ｓ１０２〕認証子の転置処理を行う。すなわち、図７のステップＳ７４で求められた内積列ＭＳ２１に基づいて、認証子Ｓ２１の転置処理を行う。具体的には、図５に示す転置処理によって認証子Ｓ２１の転置処理を行う。

【００５３】次に、本発明の他の実施例について説明する。図１１は他の端末認証手段の構成を示すブロック図である。図２と異なる点は、乱数発生手段１１ｂと演算手段１１ｄとの間に前処理手段１１ｈが追加されていることである。

【００５４】この前処理手段１１ｈは、秘密鍵データベース１１ａから移動端末局２１，２２，・・・，２ｎに対応する秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎを取得する。そして、この秘密鍵Ｋ２１，Ｋ２２，・・・，Ｋ２ｎに基づいて、図５に示す処理手順で転置処理を行い、乱数発生手段１１ｂから出力された乱数列Ｒ１，Ｒ２，・・・，Ｒｎの符号列を入れ換える。

【００５５】図１２は他の認証子発生手段の構成を示すブロック図である。図２と異なる点は、入力手段２１ｂａと演算手段２１ｂｂとの間に前処理手段２１ｂｆが追加されていることである。

【００５６】この前処理手段２１ｂｆは、秘密鍵データ２１ｂｃに基づいて、図５に示す処理手順で転置処理を行い、乱数発生手段２１ｂａで受信された乱数列Ｒ１の符号列を入れ換える。

【００５７】したがって、認証子Ｓ２１等の符号列が傍受されても、上記図１１及び図１２に示す転置処理によって、その内容を解析することはより困難になるので、通信内容の秘密性を確保することができる。

【００５８】図１３は無線基地局側の他の処理手順を示すフローチャートである。図において、Ｓの後に続く数字はステップ番号を示す。なお、ここでは図６と同様に、無線基地局１０と移動端末局２１との間の処理手順について説明する。

〔Ｓ１３１〕乱数列を発生する。具体的には、図２に示す乱数発生手段１１ｂによって乱数列Ｒ１を発生し、出力手段１１ｃによって所定の出力レベルに増幅して出力する。

〔Ｓ１３２〕ステップＳ１３１で発生した乱数列を送信する。すなわち、ディジタルデータとしての乱数列Ｒ１を、図１の通信手段１２が無線電波に変換して出力する。〔Ｓ１３３〕認証子を受信する。ステップＳ１３２で出力された乱数列Ｒ１を移動端末局２１が受信すると、認証子Ｓ２１を演算して無線電波で送信する。このため、移動端末局２１から送信された認証子Ｓ２１を受信する。

〔Ｓ１３４〕秘密鍵を取得する。具体的には、図２の秘密鍵データベース１１ａから通信の対象となる移動端末局２１に対応した秘密鍵Ｋ２１を取得する。

〔Ｓ１３５〕前処理を行う。具体的には、ステップＳ１３１で発生した乱数列Ｒ１について、後述する図１５に示す転置処理を行う。

〔Ｓ１３６〕内積演算を行う。具体的には、図８に示す処理手順と同様に、ステップＳ１３５の前処理を行なった乱数列Ｒ１と、ステップＳ１３４で取得した秘密鍵Ｋ２１とから内積を演算して、内積列ＭＳ１１を求める。

〔Ｓ１３７〕後処理を行う。具体的には、ステップＳ１３６で求められた内積列ＭＳ１１に基づいて、図９に示す抽出処理又は図１０に示す転置処理を行なって、認証子Ｓ１１を求める。

〔Ｓ１３８〕受信認証子との比較を行う。すなわち、ステップＳ１３３で受信した移動端末局２１の認証子Ｓ２１と、ステップＳ１３７で求められた認証子Ｓ１１とを比較する。

〔Ｓ１３９〕移動端末局２１が無線基地局１０に正規に登録された端末局か否かを判別する。具体的には、ステップＳ１３３で受信した移動端末局２１の認証子Ｓ２１と、ステップＳ１３７で求められた認証子Ｓ１１とが一致するか否かを判別する。もし、認証子Ｓ２１と認証子Ｓ１１とが一致する（ＹＥＳ）ならば本処理手順を終了し、そうでない（ＮＯ）ならばステップＳ１３１に戻る。

【００５９】図１４は移動端末局側の他の処理手順を示すフローチャートである。なお、ここでは図７の処理手順と同様に、認証子発生手段２１ｂの処理手順について説明する。図において、Ｓの後に続く数字はステップ番号を示す。

〔Ｓ１４１〕乱数列を受信する。すなわち、図１の無線基地局１０から送信された乱数列Ｒ１を通信手段２１ａが受信し、図３の入力手段２１ｂａがこの乱数列Ｒ１を受ける。

〔Ｓ１４２〕秘密鍵を取得する。具体的には、図３の演算手段２１ｂｂが秘密鍵データ２１ｂｃを取得する。なお、この秘密鍵データ２１ｂｃは、図６のステップＳ６４で示した移動端末局２１に対応する秘密鍵Ｋ２１と同一のデータである。

〔Ｓ１４３〕前処理を行う。具体的には、ステップＳ１４１で受信した乱数列Ｒ１について、後述する図１５に示す転置処理を行う。

〔Ｓ１４４〕内積演算を行う。具体的には、図８に示す処理手順と同様に、ステップＳ１４３で前処理した乱数列Ｒ１と、ステップＳ１４２で取得した秘密鍵データ２１ｂｃとから内積を演算して、内積列ＭＳ２１を求める。

〔Ｓ１４５〕後処理を行う。具体的には、ステップＳ１４４で求められた内積列ＭＳ２１に基づいて、図９に示す抽出処理又は図１０に示す転置処理を行なって、認証子Ｓ２１を求める。

〔Ｓ１４６〕ステップＳ１４５で求められた認証子Ｓ２１を送信する。すなわち、ディジタルデータとしての認証子Ｓ２１を、通信手段２１ａが無線電波に変換して出力する。

【００６０】次に、上記図１３及び図１４に示す前処理の具体的な処理手順について、図１５で説明する。なお、これらの図面の説明では、図１４と同様に移動端末局２１において行われる処理手順について説明する。

【００６１】図１５は前処理の処理手順を示すフローチャートである。図において、Ｓの後に続く数字はステップ番号を示す。

〔Ｓ１５１〕秘密鍵を取得する。具体的には、図３の演算手段２１ｂｂが秘密鍵データ２１ｂｃを取得する。なお、この秘密鍵データ２１ｂｃは、図６のステップＳ６４で示した移動端末局２１に対応する秘密鍵Ｋ２１と同一のデータである。

〔Ｓ１５２〕転置処理を行う。すなわち、図１４のステップＳ１４１で受信された乱数列Ｒ１について、転置処理を行う。具体的には、図５に示す転置処理に基づいて、乱数列Ｒ１の符号列を入れ換える。

【００６２】上記の説明では、無線基地局１０から移動端末局２１へ乱数列Ｒ１を送信し、移動端末局２１が認証子Ｓ２１を無線基地局１０へ送信して認証を行うように構成したが、移動端末局２１の認証子発生手段２１ｂに乱数列Ｒ２１を発生する乱数発生手段を設けて、移動端末局２１から無線基地局１０へ乱数列Ｒ２１及び認証子Ｓ２１を送信し、無線基地局１０が移動端末局２１へ認証を行うように構成することもできる。

【００６３】同様に、無線基地局１０から移動端末局２２，・・・，２ｎへ乱数列Ｒ２，・・・，Ｒｎを送信し、移動端末局２２，・・・，２ｎがそれぞれ認証子Ｓ２２，・・・，Ｓ２ｎを無線基地局１０へ送信して認証を行うように構成したが、移動端末局２２，・・・，２ｎの認証子発生手段２２ｂ，・・・，２ｎｂにそれぞれ乱数列Ｒ２２，・・・，Ｒ２ｎを発生する乱数発生手段を設けて、移動端末局２２，・・・，２ｎから無線基地

15

局１０へ乱数列Ｒ２２，・・・，Ｒ２ｎ及び認証子Ｓ２１，Ｓ２２，・・・，Ｓ２ｎをそれぞれ送信し、無線基地局１０が移動端末局２２，・・・，２ｎへ認証をそれぞれ行うように構成することもできる。

【００６４】こうすることによって、無線基地局１０から移動端末局２１等へ、又は移動端末局２１等から無線基地局１０へ自在に認証を求めることができる。

【００６５】

【発明の効果】以上説明したように本発明では、まず無線基地局の端末認証手段で発生した乱数列を第１の無線通信手段が送信するとともに、この乱数列と移動端末局に対応する秘密鍵とから第１の認証子を求め、また乱数列を受信した移動端末局の認証子発生手段がこの乱数列と移動端末局自身の秘密鍵とから第２の認証子を求めて第２の無線通信手段が送信し、さらに移動端末局から送信された第２の認証子を受信した無線基地局の端末認証手段が上記第１の認証子と比較して所定の許否信号を出力するように構成したので、従来の携帯用無線通信装置であっても暗号化及び復号化処理が短時間で行え、移動端末局の認証を行うことができる。

【００６６】また、無線基地局と移動端末局との間で送受信される乱数列等のデータが他の無線機等で傍受されても、抽出処理又は転置処理を行なっているので復号化が複雑なため、移動端末局の認証で安全に使用することができる。

【００６７】さらに、専用のハードウェアを必要としないので、コストを低く抑えることができる。

【図面の簡単な説明】

【図１】本発明の原理説明図である。

【図２】端末認証手段の構成を示すブロック図である。

【図３】認証子発生手段の構成を示すブロック図である。

16

【図４】認証子の決定方法の一例を示す図であり、（Ａ）には内積列の一例を示し、（Ｂ）には鍵と認証子との関係を示す。

【図５】転置処理の一例を示す図である。

【図６】無線基地局側の処理手順を示すフローチャートである。

【図７】移動端末局側の処理手順を示すフローチャートである。

【図８】内積演算の処理手順を示すフローチャートである。

【図９】後処理の処理手順を示すフローチャートである。

【図１０】他の後処理の処理手順を示すフローチャートである。

【図１１】他の端末認証手段の構成を示すブロック図である。

【図１２】他の認証子発生手段の構成を示すブロック図である。

【図１３】無線基地局側の他の処理手順を示すフローチャートである。

【図１４】移動端末局側の他の処理手順を示すフローチャートである。

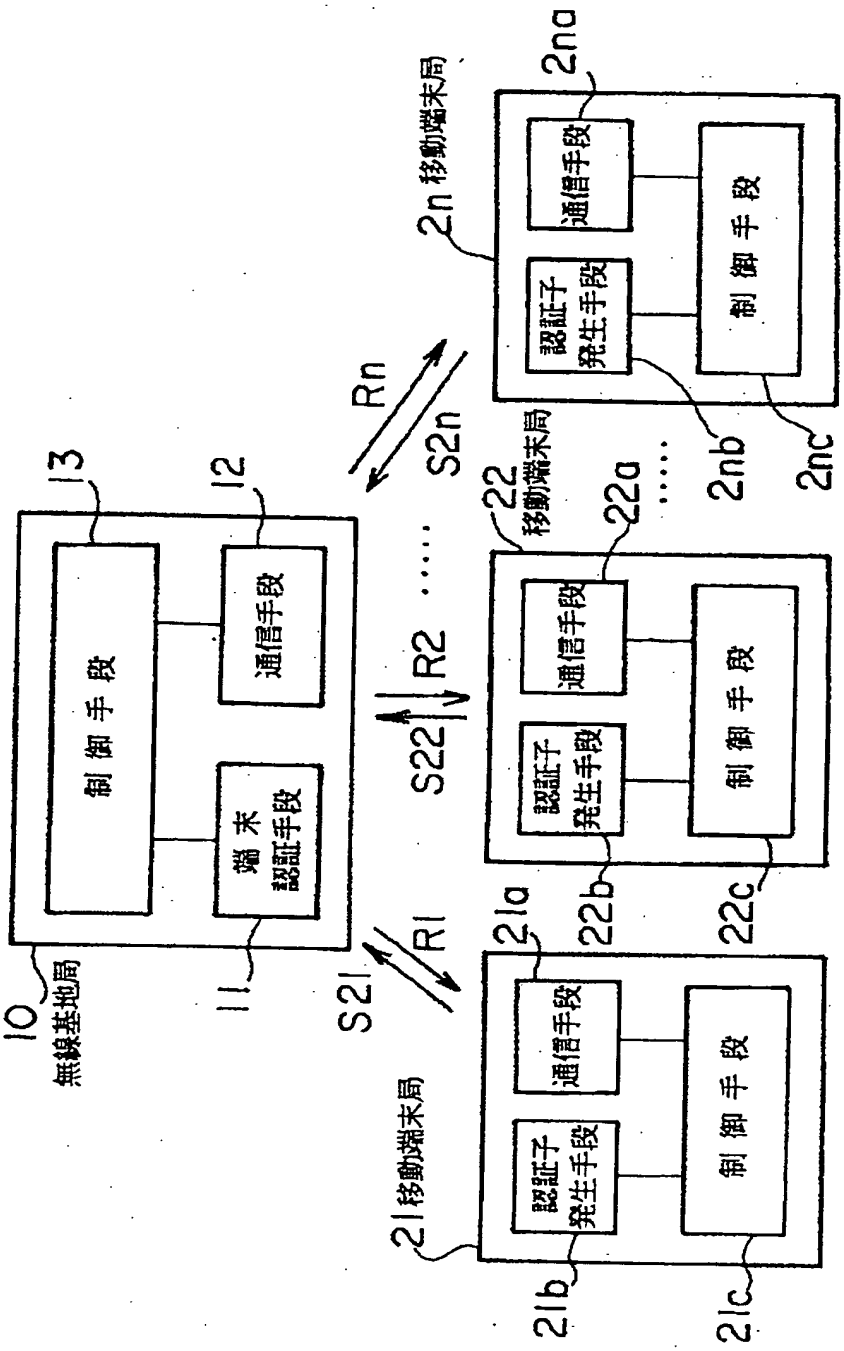
【図１５】前処理の処理手順を示すフローチャートである。

【符号の説明】

１０　無線基地局
１１　端末認証手段
１２　第１の無線通信手段
２１，２２，・・・，２ｎ　移動端末局
２１ａ，２２ａ，・・・，２ｎａ　第２の無線通信手段
２１ｂ，２２ｂ，・・・，２ｎｂ　認証子発生手段

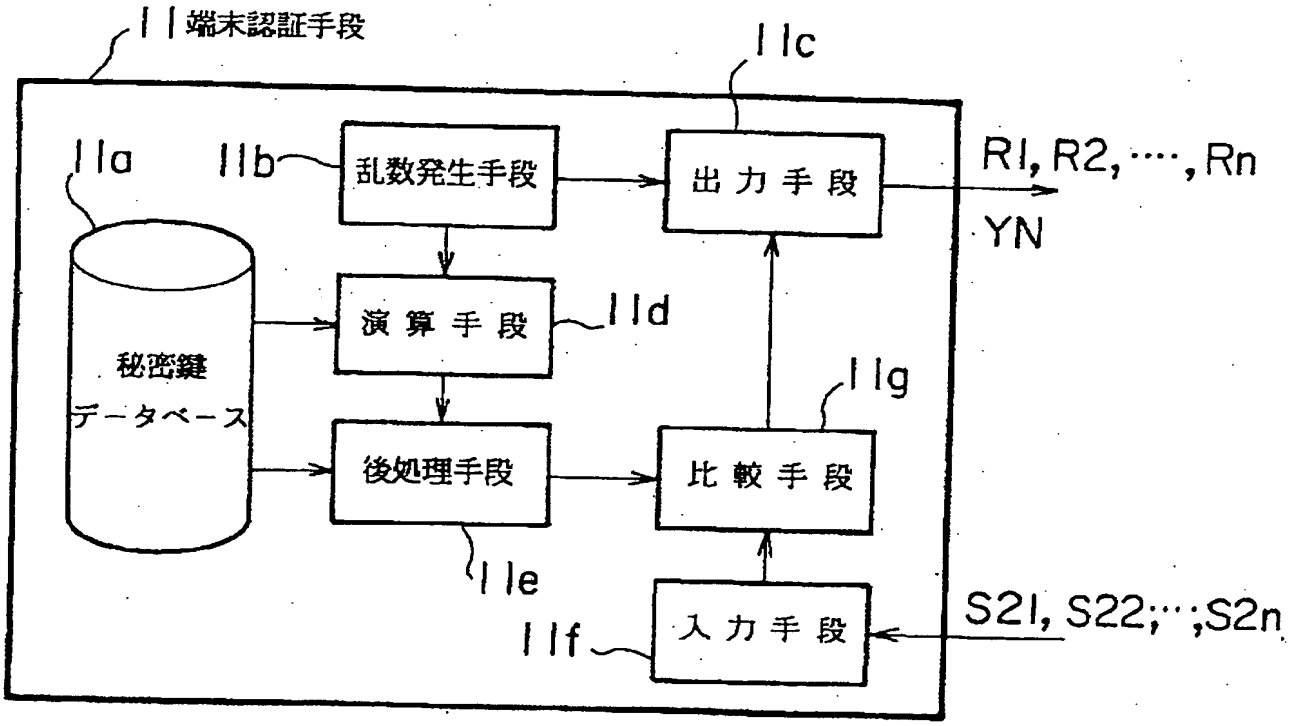
【図1】

本発明の原理説明図



【図2】

端末認証手段の構成を示すブロック図



【図5】

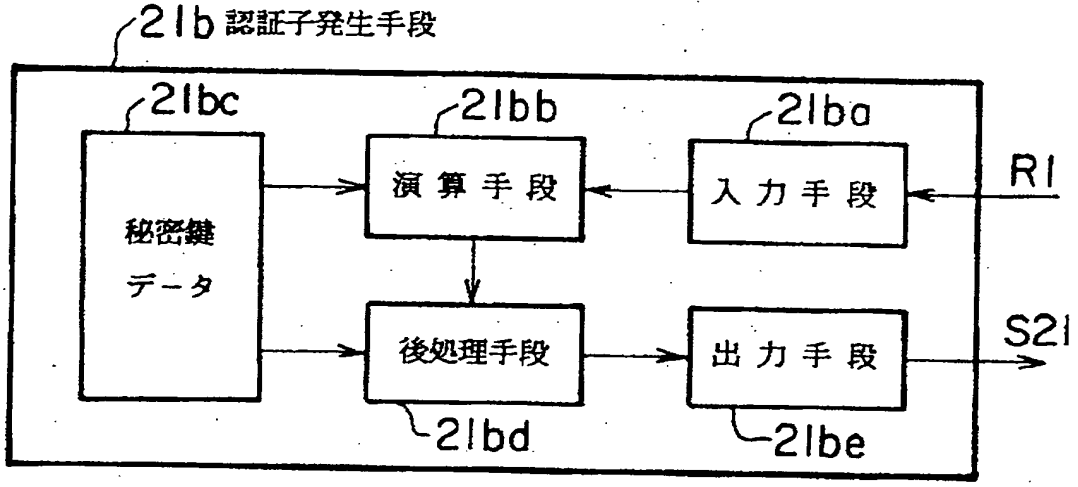
転置処理の一例を示す図

400転置処理表

	鍵データ	転置前データ	転置後データ
401	001	$B_7 B_6 B_5 B_4 B_3 B_2 B_1 B_0$	B_6
402	001	$B_7 B_5 B_4 B_3 B_1 B_0$	$B_5 B_3$
	101	$B_7 B_4 B_3 B_2 B_1 B_0$	$B_5 B_3 B_0$
	110	$B_7 B_4 B_3 B_2 B_1$	$B_6 B_5 B_3 B_4$
403	10	$B_7 B_3 B_2 B_1$	$B_6 B_5 B_3 B_4 B_2$
	10	$B_7 B_3 B_1$	$B_6 B_5 B_3 B_4 B_2 B_0$
	1	$B_7 B_1$	$B_6 B_5 B_3 B_4 B_2 B_1 B_0$
404			$B_6 B_5 B_3 B_4 B_2 B_1 B_0 B_7$

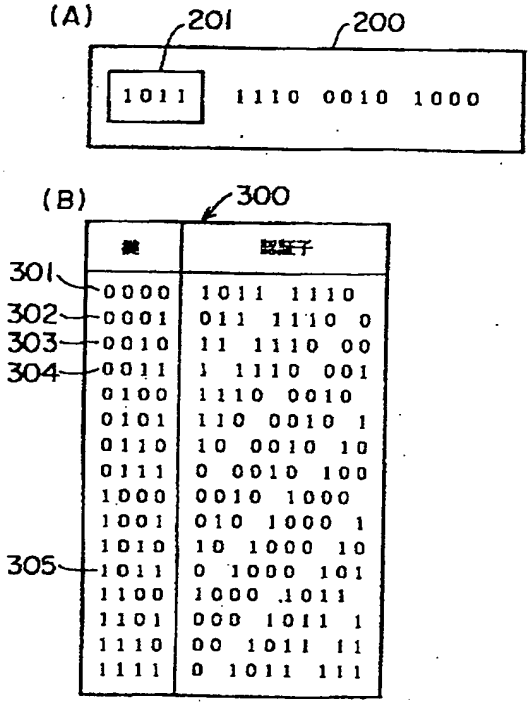
【図3】

認証子発生手段の構成を示すブロック図



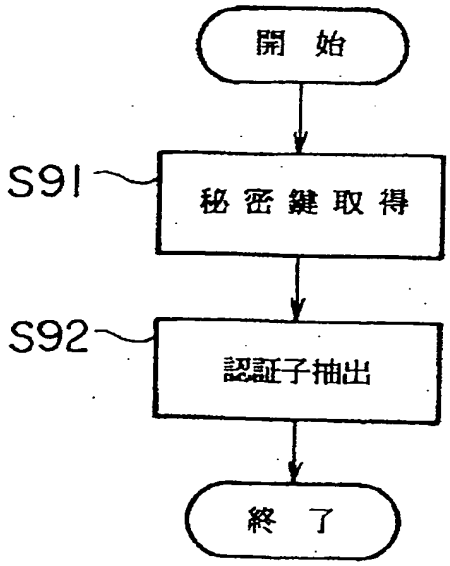
【図4】

認証子の決定方法の一例を示す図

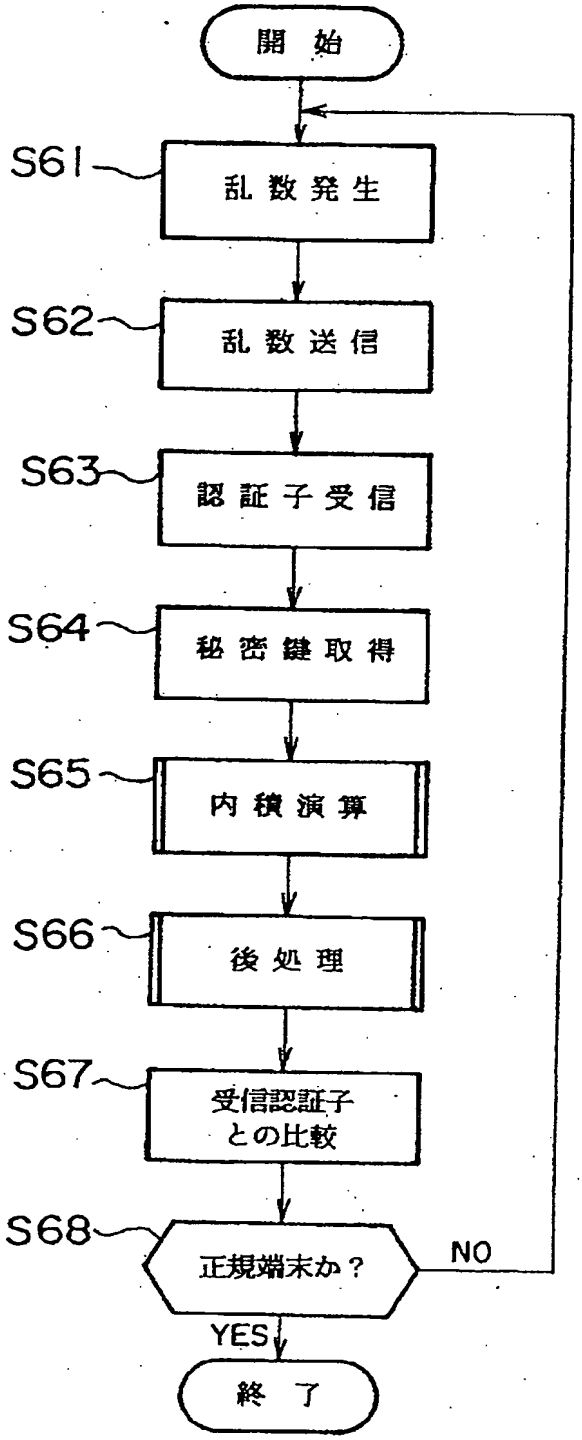


【図9】

後処理の処理手順を示すフローチャート



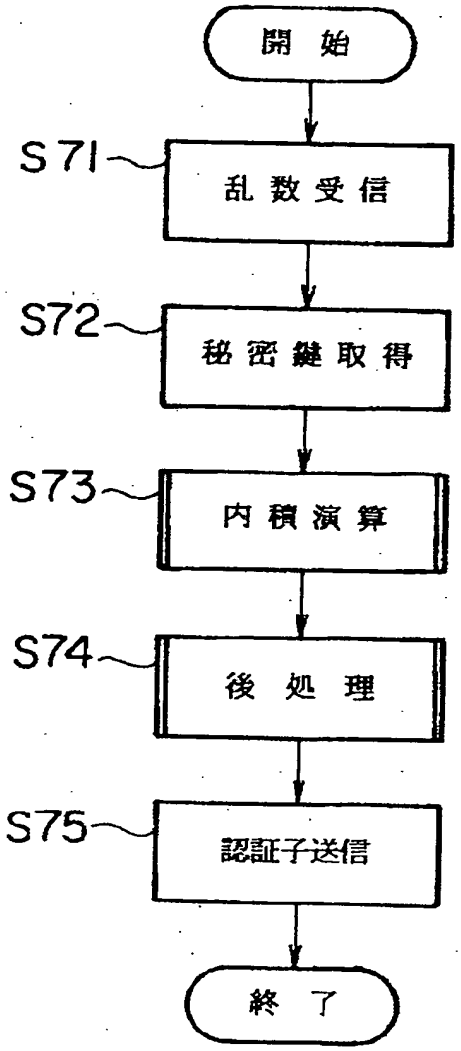
【図6】



無線基地局側の
処理手順を示す
フローチャート

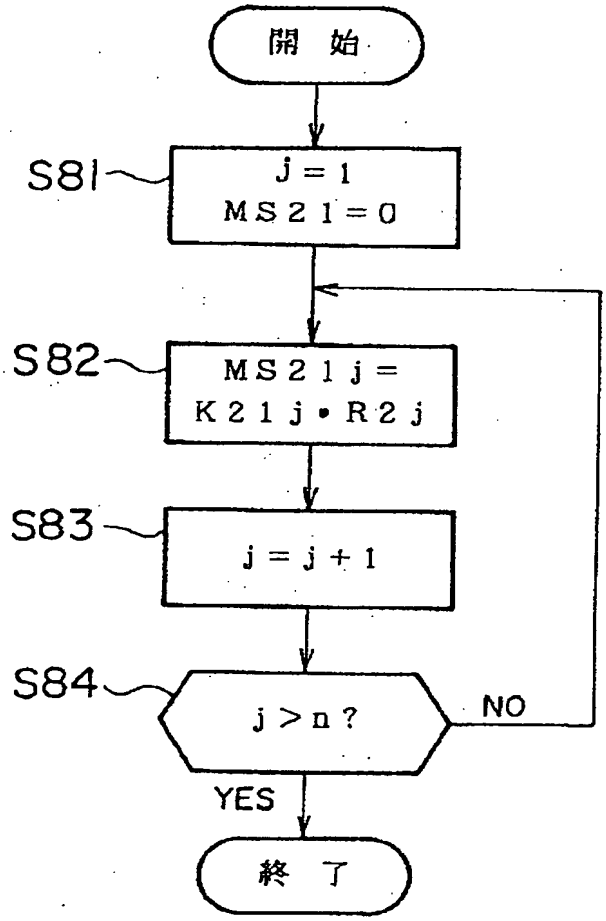
【図7】

移動端末局側の処理手順を示すフローチャート



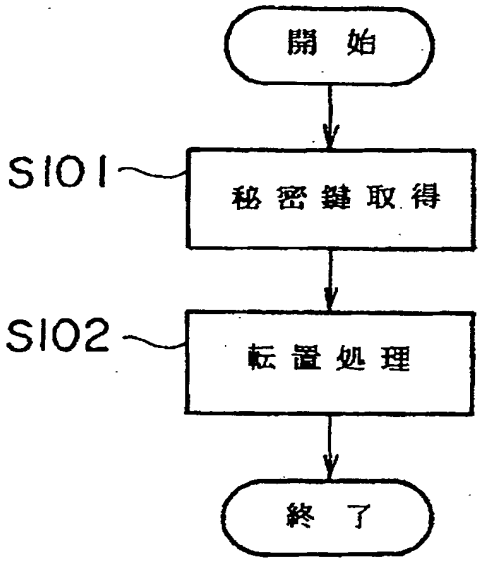
【図8】

内積演算の処理手順を示すフローチャート



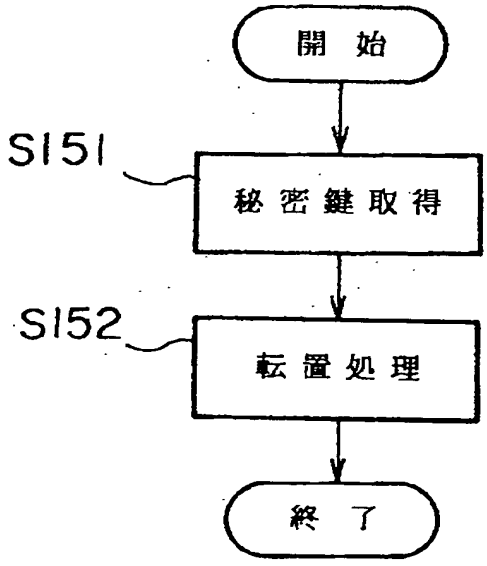
【図10】

他の後処理の処理手順を示すフローチャート



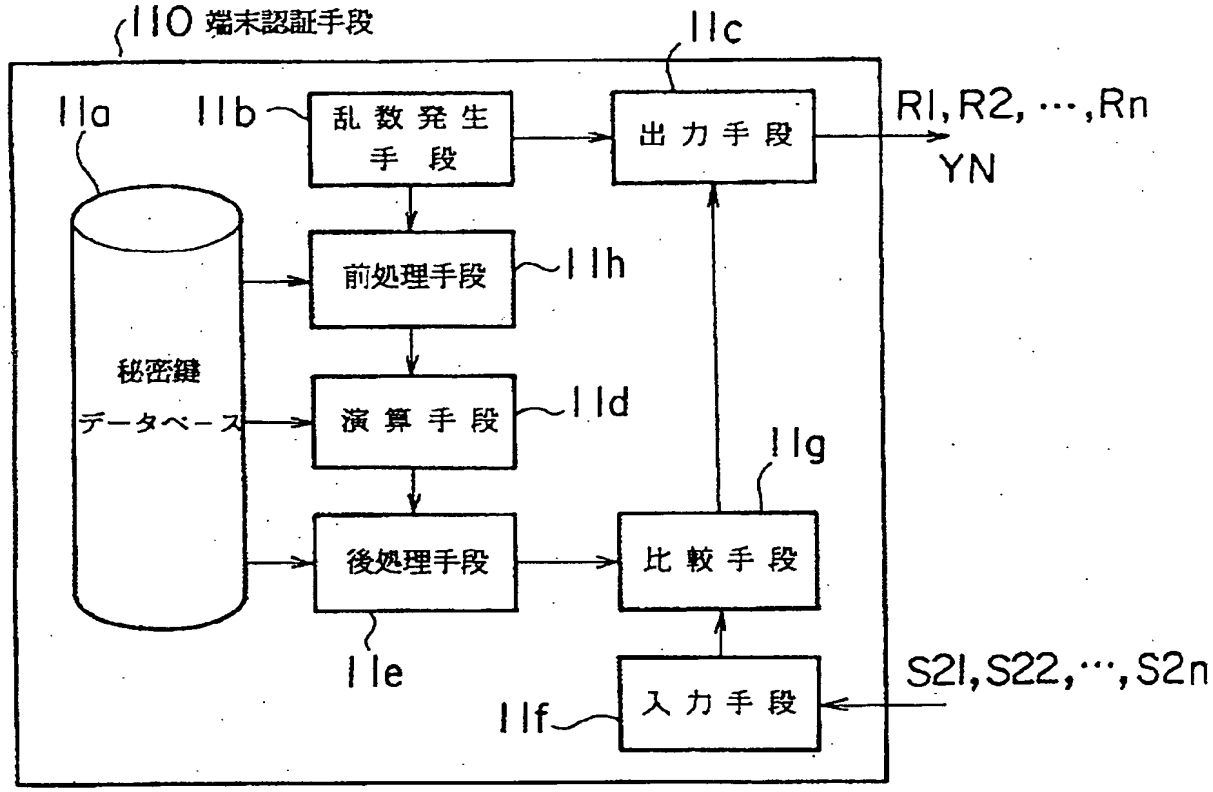
【図15】

前処理の処理手順を示すフローチャート



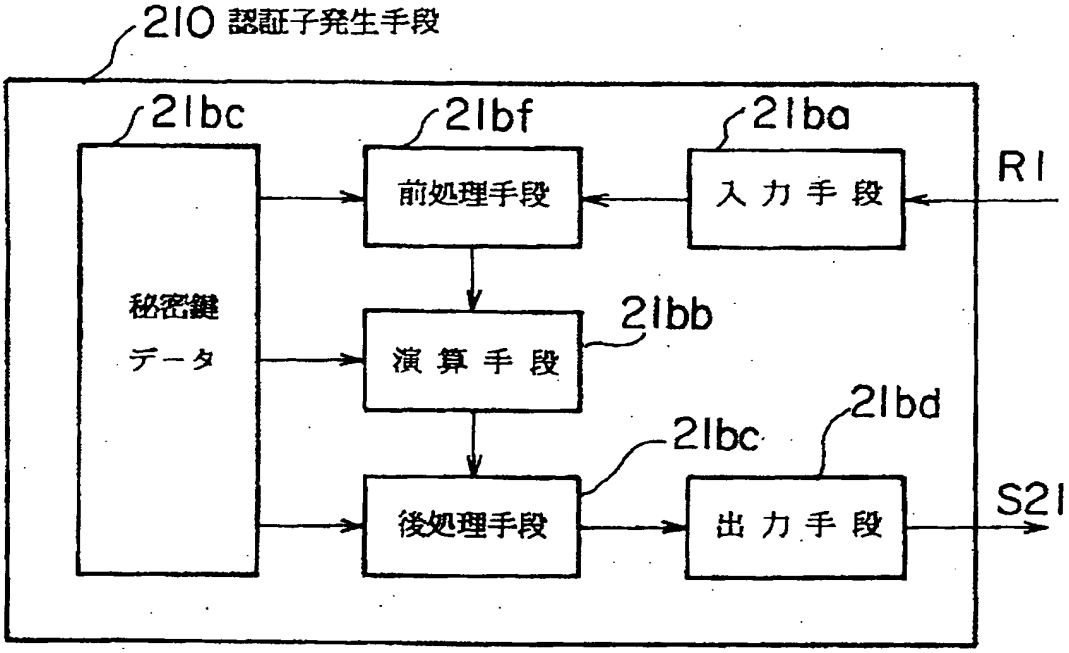
【図11】

他の端末認証手段の構成を示すブロック図



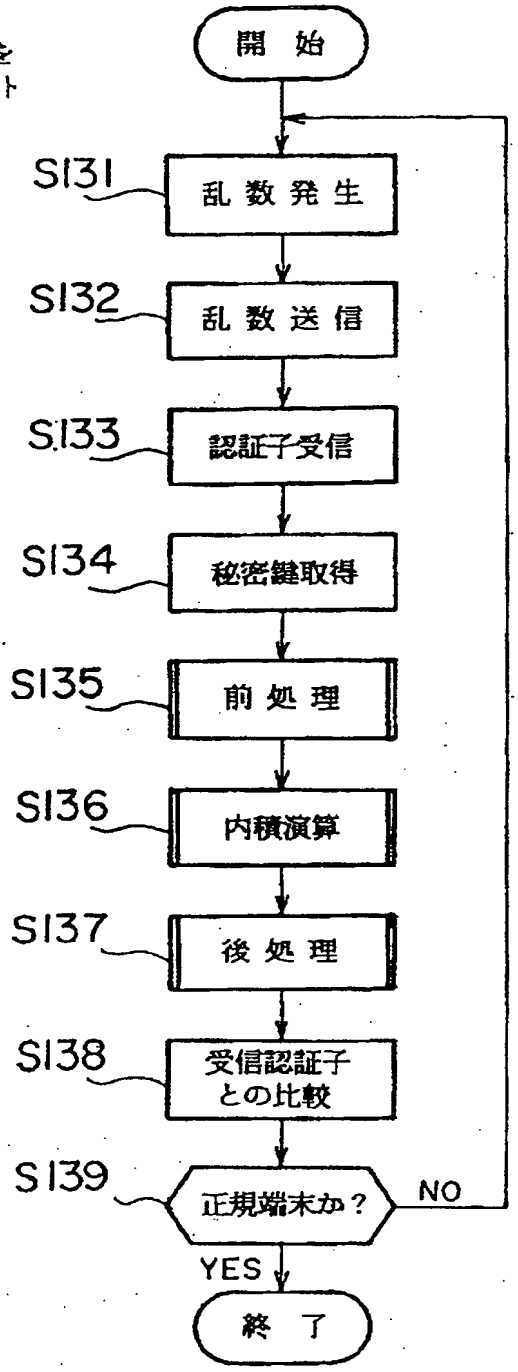
【図12】

他の認証子発生手段の構成を示すブロック図



【図13】

無線基地局側の他の処理手順を示すフローチャート



【図14】

移動端末局側の他の処理手順を示すフローチャート